



# Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 09 June 2005

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Houston Chronicle reports immigration officials hope to expand the Expedited Removal program, which should help to reduce the number of illegal immigrants who disappear within the country. (See item [8](#))
- CBS reports at least eight California Amtrak Capitol Corridor trains have been delayed and Bay Area Rapid Transit service disrupted while a bomb squad combs through an Amtrak train forced to stop because of a passenger's suspicious behavior. (See item [9](#))
- The Associated Press reports federal authorities have detained four men who they believe are linked to an al Qaeda terror cell, in Lodi, California. (See item [30](#))

### DHS/IAIP Update Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Products & Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *June 08, Charlotte Observer (NC)* — **Duke Power starts tests of mixed-oxide fuel.** Duke Power has officially begun its tests of mixed-oxide, or MOX, fuel, which contains surplus weapons plutonium, at its Catawba nuclear plant on Lake Wylie in South Carolina. A Catawba reactor loaded with four MOX fuel assemblies, among 189 conventional assemblies, was restarted on Monday, June 6, said Duke spokesperson Rita Sipe. It will take a few days for the reactor to reach full power. With that, Catawba becomes the first commercial power plant to

make electricity from weapons plutonium. The fuel blends five percent plutonium oxides with 95 percent uranium oxides. A slightly different version of MOX that doesn't use weapons-grade plutonium has been used in European power plants for more than 20 years. Duke intends to test MOX at Catawba for about 4 1/2 years. The fuel will be examined when the reactor is shut down for refueling about every 18 months. The tests are intended to confirm that the fuel behaves much like the enriched-uranium fuel commonly used in U.S. power plants.

Source: [http://www.charlotte.com/mld/charlotte/news/11840541.htm?source=rss&channel=charlotte\\_business](http://www.charlotte.com/mld/charlotte/news/11840541.htm?source=rss&channel=charlotte_business)

2. *June 07, Associated Press* — **Utilities rely on voluntary conservation programs.** Many states and electric utilities see voluntary residential rate reduction programs as providing a critical cushion, even if they can't prevent a major outage like the Northeast blackout in 2003. "You'll find that (home systems) can respond pretty quick, as opposed to a manufacturing plant, which needs hours to crank something down," said Ross Malme, chief executive of Retx Inc., a provider of energy communications technology. "The faster a consumer can respond to an event, the more valuable they become," said Malme. At least five million U.S. homes are enrolled in conservation programs, some of which have been around since the 1970's. Interest waned, however, until soaring demand, rising prices and the major outages of recent years exposed the system's vulnerability. People who sign up let their utility install a small device with which the company can remotely control their central air conditioning units and swimming pool pumps, another major power drain. Residential conservation also lets utilities avoid buying extra power to cover shortages. Excess capacity can cost several times the normal price in the wholesale market, and that expense can trickle down to consumers.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/06/07/AR2005060701212.html>

3. *June 07, Associated Press* — **Hope Creek nuclear plant shut down.** The operators of the Hope Creek nuclear power plant have shut it down because of a leak inside the plant's drywell. Workers manually closed down the plant at about 2:15 p.m. on Tuesday, June 7, after noticing that the leakage exceeded five gallons per minute, according to PSEG Nuclear, which operates the plant. There was no release of radiation. Plant personnel were planning to enter the drywell to determine the source of the leak. PSEG spokesperson Skip Sindoni said it was too early to estimate when the plant might go back online. The Hope Creek plant is one of three nuclear reactors, along with Salem 1 and 2, that PSEG Nuclear operates at a complex in Lower Alloways Creek Township in Salem County, NJ, along the Delaware River.

Source: <http://www.phillyburbs.com/pb-dyn/news/104-06072005-499567.html>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

Nothing to report.

[\[Return to top\]](#)

## **Banking and Finance Sector**

4. *June 08, Associated Press* — **Terror financing, anti–money laundering experts gather in Asia.** Terror financing and anti–money laundering experts from over 30 nations began meeting in Singapore on Wednesday, June 8, with several Southeast Asian countries expected to outline new measures to prevent the bankrolling of militant activities in the region. More than 400 officials and experts on terror financing are expected to attend the three–day conference. Malaysia, Indonesia, Thailand and the Philippines will outline their policies to prevent money laundering and measures to combat terror funding, according to a statement. The conference is organized by the Financial Action Task Force, a 33–member group founded in 1987 to monitor and fight money laundering, and in 2001 expanded its role to combat financing of terrorist activities.

Financial Action Task Force: <http://www.fatf-gafi.org/>

Source: <http://asia.news.yahoo.com/050608/ap/d8aj8up83.html>

5. *June 07, IT–Observer* — **U.S. companies will monitor employee e–mail.** Growing concern over sensitive information leaving the enterprise through outbound e–mail forces technology decision–makers at large and small U.S. companies to employ people to monitor outbound e–mail for legal and financial information. A recent survey results, conducted by Proofpoint, indicate the rising prominence of outbound email as a source of risk for corporations. US companies are most concerned about ensuring that email isn't used to leak company secrets and confidential information. The results also highlighted an increasingly concern about compliance with healthcare and financial regulations. The survey found that more than 63% of U.S. corporations with 1,000 or more employees either employ or plan to employ staff to read or otherwise analyze outbound e–mail.

More information about the survey is available at:

<http://www.proofpoint.com/id/outbound/index.php?id=>

Source: <http://www.ebcvg.com/articles.php?id=755>

[\[Return to top\]](#)

## **Transportation and Border Security Sector**

6. *June 08, CNN* — **Report: FAA oversight lagging behind industry changes.** The Federal Aviation Administration (FAA) isn't doing enough to adapt its safety oversight and inspection plans to respond to changes in the aviation industry, said a report released Wednesday, June 8. "During the past four years, network air carriers have faced record financial losses and made unprecedented changes to their operations to regain profitability," said the report from the inspector general's office in the Department of Transportation. Network air carriers have struggled, while low–cost ones have grown, introducing a different industry requiring a "dynamic oversight process," the report said. "The FAA has made progress in moving to a more risk–based, data–driven air carrier oversight system designed to respond to the types of changes

occurring in the industry. However, the FAA still has a substantial amount of work ahead to improve its oversight systems, especially given the magnitude of changes air carriers are making and the pace at which the changes are occurring." The agency's oversight of airlines is inconsistent, the report said. Inspectors increased oversight on three airlines that were in or near bankruptcy, but they didn't for two other major carriers, even though all five were making similar changes to their systems. The report made 10 recommendations for the FAA. The agency has agreed to implement five of those recommendations and will partially implement others.

Report: <http://www.oig.dot.gov/item.jsp?id=1575>

Source: <http://www.cnn.com/2005/TRAVEL/06/08/aviation.safety/>

7. *June 08, Associated Press* — **Plan for voluntary Biometric ID gets first taker.** Since the federal government began letting select frequent fliers with new high-tech passes speed through airport security checkpoints, one of the biggest complaints has been that the year-old program is too limited to be of much use. Now, a privately run version coming online in Florida could spur efforts to broaden the program. Beginning June 21, the Orlando airport will let travelers pay \$80 a year for a card that guarantees an exclusive security line and the promise of no random secondary pat down. To get this new "Clear" card, travelers would have to be vetted by the Department of Homeland Security and submit to fingerprint and iris scans. Similar systems exist at some European airports, and in five U.S. airports as part of a test by the Transportation Security Administration (TSA). But the TSA's "Registered Traveler" program, which is free for now while in its test phase, has been capped at 10,000 participants, and cards obtained at one airport don't work at others. The TSA is open to broadening Registered Traveler through public-private partnerships, and several airports have expressed interest, said Steve Van Beek, executive vice president of policy for Airports Council International, a trade association. But he is concerned that the concept could run aground unless the TSA enforces technology standards that enable cards to work at more than one airport.

Source: <http://www.informationweek.com/showArticle.jhtml;jsessionid=0SPBQ05DCVYVUQSNDBCKKH0CJUMKJVN?articleID=164301373>

8. *June 08, Houston Chronicle* — **Immigration officials seek expansion of program to deport illegal immigrants quickly.** U.S. immigration officials said Tuesday, June 7, they hope to expand a program that allows Border Patrol officers to deport illegal immigrants without taking them before a judge. Used at two of the 20 crossings along the Mexican border, the process called Expedited Removal may soon include all southern Border Patrol areas, said Wesley Lee, acting director of detention and removal operations at the Department of Homeland Security. Expanding the program will help to reduce the number of illegal immigrants who disappear within the country, said Stewart Verdery, adjunct fellow at the Center for Strategic and International Studies. Border Patrol agents can use the process to send Mexican immigrants home quickly, but they more often apply it to immigrants from other countries who enter the United States from Mexico through Laredo, TX, and Tucson, AZ, as well as between ports of entry. This year, 98,000 of the 800,000 illegal immigrants caught by Border Patrol officials were from countries other than Mexico. "(They) represent a massive new wave in migrants that bring significant concerns that nationals from countries with more terrorism activity than Mexico may be utilizing the southern border to enter the U.S.," Verdery said.

Source: [http://www.mywesttexas.com/site/news.cfm?newsid=14659727&BRD=2288&PAG=461&dept\\_id=547111&rfti=6](http://www.mywesttexas.com/site/news.cfm?newsid=14659727&BRD=2288&PAG=461&dept_id=547111&rfti=6)

9. *June 08, CBS (CA)* — **Bay Area Amtrak, Bart Station shut down.** At least eight California Amtrak Capitol Corridor trains have been delayed and Bay Area Rapid Transit (BART) service disrupted on Wednesday, June 8, while a bomb squad combs through an Amtrak train forced to stop in Richmond because of a passenger's suspicious behavior, an Amtrak spokesperson said. Amtrak's Vernae Graham said train No. 525 from Sacramento to Oakland stopped in Richmond around 7:45 a.m. after a passenger who missed the Martinez stop "became irate and started ranting and yelling, enough so that the train personnel called the local law enforcement agencies." Richmond police Sgt. Mark Gagan said the man told police the same thing he told conductors, that the train would "fall into the sea" and "disappear." After one of the packages the man was carrying was deemed suspicious, more than 100 passengers were evacuated and the Richmond station shut down. The man allegedly made comments to conductors about being Muslim and began "chanting and praying in a foreign language," Gagan said. His "demeanor was very nervous and awkward, he was fidgety and sweaty, and very agitated." Gagan described the man as apparently Middle Eastern and in his mid-30s. Investigators are concerned that he got on the train in Sacramento carrying "several" tickets, including to Martinez and to Bakersfield, and then left at least one of his packages on an upper deck of the train, far from his seat.

Source: [http://cbs5.com/localwire/localnews/bcn/2005/06/08/n/HeadlineNews/SUSPICIOUS-PASSENGER/resources\\_bcn.html](http://cbs5.com/localwire/localnews/bcn/2005/06/08/n/HeadlineNews/SUSPICIOUS-PASSENGER/resources_bcn.html)

[[Return to top](#)]

## **Postal and Shipping Sector**

10. *June 08, Seattle Times (WA)* — **U.S. postal officials mull Snohomish County anthrax plan.** U.S. Postal Service (USPS) officials are considering a Snohomish, WA, Health District proposal that would help employees receive necessary medical treatment if exposed to anthrax. The district's health board decided last month against participating in an emergency-response plan linked to anthrax-detection alarms at a postal facility in Everett, WA. The USPS is installing more than 280 biohazard-detection systems nationwide. USPS expected the local health districts to screen employees for exposure and to prescribe antibiotics in the event of an alarm. But the Snohomish Health District — as well as other health agencies nationwide — balked at what it called an unfunded mandate laden with liability issues. Not wanting the liability, the health district says it would be willing to provide a letter that employees could take to their personal physicians explaining their potential for exposure to anthrax and the need for a prescription. The prescriptions could then be held securely on file at the Everett postal facility and would be returned to employees to be filled at a pharmacy or by a doctor if needed. So it could confirm to medical facilities the names of postal employees who might be exposed, the health district also would keep on file a list of the employees. Seattle postal officials have sent the plan to USPS headquarters in Washington, DC, for consideration.

Source: [http://seattletimes.nwsources.com/html/snohomishcountynews/2002321018\\_anthrax08m.html](http://seattletimes.nwsources.com/html/snohomishcountynews/2002321018_anthrax08m.html)

11. *June 07, WBAY (WI)* — **Green Bay post office receives detection equipment.** Green Bay, WI's main post office is getting new high-tech equipment this month to detect anthrax in letters before they leave the post office. The \$200,000 biohazard detection system attaches to the

machine that cancels stamps, and automatically analyses mail for anthrax or other biological agents, though the U.S. Postal Service says its focus is catching anthrax. The system will be operational on June 25. The biohazard detection system is already at post offices in Milwaukee, Madison, and La Crosse.

Source: <http://www.wbay.com/Global/story.asp?S=3444022&nav=51s7alLW>

[[Return to top](#)]

## **Agriculture Sector**

12. *June 06, New York Newsday* — **Red tide spreads to Martha's Vineyard.** Environmental officials closed two areas off Martha's Vineyard to shellfishing on Monday, June 6, as the largest red tide outbreak in decades continued its spread through New England waters. The toxic algae bloom already has forced officials to shut down shellfish beds from Maine to Cape Cod, MA. The closures off Edgartown meant the outbreak was continuing south, scientists said. Scientists say the algae contaminate only shellfish, making them unsafe for animals and humans to eat. This year, strong east and northeast winds, including two May nor'easters, blew in a particularly heavy algae bloom that flourished in warmer coastal waters. The outbreak is the worst to hit Massachusetts since 1972, when the state enacted a blanket closure of all shellfish beds.

Source: <http://www.newsday.com/news/local/wire/connecticut/ny-bc-ct--redtide0606jun06%2C0%2C4844138%2Cprint.story>

[[Return to top](#)]

## **Food Sector**

13. *June 07, Associated Press* — **Scientific paper on milk supply delayed for security reasons.** The National Academy of Sciences has delayed publication of a research paper at the request of the Department of Health and Human Services (HHS), which was concerned that the material might be useful to terrorists. The paper, assessing the vulnerability of the dairy industry to bioterror attack and recommending steps to prevent that from happening, had been scheduled for publication May 30. A notice of upcoming reports in the journal Proceedings of the National Academy of Sciences briefly listed the paper, but it was withdrawn after HHS raised concerns, William Kearney, director of media relations for the academy, said Tuesday, June 7. In a letter to the Academy, Stewart Simonson, assistant secretary of HHS, charged that the paper was a "road map for terrorists." Simonson contended that the paper provided too much detail on potentially vulnerable areas of the milk supply, processing and distribution systems and argued that its publication "could have very serious health and national security consequences."

Source: [http://www.nctimes.com/articles/2005/06/08/special\\_reports/science\\_technology/16\\_53\\_576\\_7\\_05.txt](http://www.nctimes.com/articles/2005/06/08/special_reports/science_technology/16_53_576_7_05.txt)

[[Return to top](#)]

## **Water Sector**



14. *June 06, KKWL (IA)* — **Nitrate levels in Iowa drinking water source raise concern.** More than 125,000 Eastern Iowans depend on the Cedar River for drinking water, but state environmentalists say it's getting more and more polluted. Nitrate levels in the Cedar River have been gradually increasing over the years. Black Hawk County Health officials say something needs to be done to reduce potential health risks. Mark Linda with the Black Hawk County Health Department said, "nitrates are a problem for infants under three months of age. There are other studies that have found nitrates having an impact on pregnant females." The Iowa Department of Natural Resources is asking farmers to carefully monitor how much nitrogen fertilizer they use. State lawmakers say monitoring the river is a start to solving this long-term problem. State representative Don Shoultz said, "we did pass legislation this last year that would put five million dollars in a water quality program. It's going to be a start, but we're going to have to put a significant amount of money into it." This issue is of critical importance to Cedar Rapids, because the city gets its drinking water from shallow wells along the Cedar River.

Source: <http://www.kwwl.com/Global/story.asp?S=3438464&nav=2IfuaiOa>

[[Return to top](#)]

## **Public Health Sector**

15. *June 08, Reuters* — **Call for three billion dollars to fund neglected disease research.**

Governments around the world should provide three billion dollars a year to fund research into neglected diseases, a group of leading scientists and charities said on Wednesday, June 8. According to the Drugs for Neglected Diseases Initiative, a mere 10 percent of health research resources go into diseases accounting for 90 percent of the global disease burden. Infectious diseases that kill millions of people in the developing world every year have long been ignored by Western firms, because medicines to fight them make no money. Recently a number of non-profit groups have been established to kickstart research into areas such as malaria and tuberculosis. They want world leaders, meeting next month at the G8 summit in Scotland, to make research into neglected diseases a priority. In addition to extra money, they are urging governments to overhaul rules to stimulate research.

Source: <http://www.alertnet.org/thenews/newsdesk/L0754039.htm>

16. *June 08, University of Illinois – Chicago* — **Prototype Severe Acute Respiratory syndrome drug.** A prototype drug created by researchers at the University of Illinois at Chicago shows promise in slowing replication of the virus responsible for Severe Acute Respiratory Syndrome (SARS). The researchers have received an \$8 million grant from the National Institute of Allergy and Infectious Diseases to develop protease inhibitors — a class of drugs capable of disrupting enzymes that digest proteins — that would block key enzymes in the SARS virus and hamper its advance. "Data from SARS patients indicate that replication of the virus peaks 10 days after the onset of fever," said Michael Johnson, the study's principal investigator. "By administering protease inhibitors early, when feverish symptoms have started, the drugs could reduce the viral load and ameliorate the disease." The SARS virus multiplies rapidly, hijacking the machinery of the cells it infects to clone itself over and over again. One of the first steps in that process is the production of a long chain of proteins, all of which are needed for the virus to propagate. Two enzymes, or proteases, clip the chain to release the individual proteins, the

parts needed to assemble a mature virus. These two proteases — called 3CLpro and PLpro — are UIC's targets for drug therapy.

Source: <http://tigger.uic.edu/htbin/cgiwrap/bin/newsbureau/cgi-bin/index.cgi?from=Releases&to=Release&id=1150&frommain=1>

17. *June 08, Hudson Valley News (NY)* — **Anthrax drill tests hospitals' resources.** Staff from 28 hospitals, in the seven county Hudson Valley region of New York, Tuesday, June 7, tested their readiness abilities with an anthrax drill. The scenario involved a fictional extremist group's intentional release of anthrax spores within the New York City regional mass transit system and commuters unknowingly carrying the illness to their hometowns. The drill was a way to test each hospital's abilities to address a bioterrorism alert. Westchester Med's Disaster Emergency Services Director Ted Tully said the exercise appears to have gone well. "We were looking to see how many patients we could take in if this was a true disaster," he said. Hospitals communicated back and forth with one another and their county health departments and emergency centers.

Source: [http://www.midhudsonnews.com/News/Anthrax\\_drill-08Jun05.htm](http://www.midhudsonnews.com/News/Anthrax_drill-08Jun05.htm)

18. *June 07, Agence France Presse* — **Indonesian polio cases rise.** Indonesia has confirmed four more cases of polio, bringing the number of children infected with the disease in the country's first outbreak in a decade to 20, a health official said. The cases were confirmed Monday, June 6, almost a week after Indonesia carried out a huge vaccination program aimed at reaching 6.4 million children under five in two days in an effort to contain the spread of the virus. All four new cases came from three districts in western part of Java island, including one in Sukabumi district where the first case of polio was detected in April, the World Health Organization said. The other victims were located in the Lebak and Cianjur districts. Indonesia plans to launch a second round of polio immunization between June 28 and 29.

Source: [http://news.yahoo.com/s/afp/20050607/hl\\_afp/healthpolioindonesia\\_050607171451;\\_ylt=Amj8Gbfo55F4.ez3QkG5pyJOrgF:\\_ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCU](http://news.yahoo.com/s/afp/20050607/hl_afp/healthpolioindonesia_050607171451;_ylt=Amj8Gbfo55F4.ez3QkG5pyJOrgF:_ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCU)

[[Return to top](#)]

## **Government Sector**

19. *June 08, Department of Homeland Security* — **Department of Homeland Security launches Listo Negocios.** The U.S. Department of Homeland Security (DHS), in partnership with the Advertising Council, on Wednesday, June 8, launched Listo Negocios. This extension of the Listo campaign, which educates and empowers Spanish-speaking individuals to prepare for and respond to potential terrorist attacks and other emergencies, focuses on business preparedness. Listo Negocios will help Spanish-speaking owners and managers of small to medium-sized businesses prepare their employees, operations and assets in the event of an emergency. One of the key findings of the 9/11 Commission report was the need for the private sector to prepare for potential disasters. An emergency preparedness plan can greatly improve the likelihood that a company will survive and recover from all emergencies, natural disasters or terrorist attacks, but, too few businesses are taking the necessary steps to prepare. Listo Negocios is the Spanish version of the Ready Business campaign, which DHS unveiled in September 2004. The list is designed to make emergency planning easier by providing



businesses with practical steps and easy to use templates in Spanish to help them plan to stay in business, talk to their employees, and protect their investment.

Listo Negocios Website (<http://www.listo.gov>)

Source: <http://www.dhs.gov/dhspublic/display?content=4534>

[[Return to top](#)]

## **Emergency Services Sector**

20. *June 08, The Herald (FL)* — **Emergency disaster drill scheduled for next week.** Airport officials at Sarasota–Manatee Airport in Sarasota, FL, will conduct an emergency disaster drill next Wednesday, June 22. The drill will involve about 300 people and take place inside the airport's fence. The drill is an opportunity for airport personnel and organizations with Sarasota and Manatee counties to practice tasks related to emergency response. The U.S. Coast Guard will provide a C–130 aircraft to simulate a passenger–aircraft emergency, with 65 passengers on board. The Sarasota–Manatee Airport Authority must conduct a full–scale exercise every three years to maintain its airport operator certificate.  
Source: <http://www.bradenton.com/mld/bradenton/11844666.htm>
21. *June 08, Associated Press* — **Pentagon holds emergency response training exercise.** A mock attack on the Pentagon and nearby office buildings took place Wednesday, June 8. The purpose was to test emergency responders. It was the third such exercise at the Pentagon since the September 11, 2001 terrorist attacks. The military called it a "full–scale response to evaluate existing plans" in response to "multiple threats." But while one victim yelled "I'm dying" and others screamed in anguish, it took at least 15 minutes for first responders to arrive. Participants said that was part of the drill, noting some units had to be kept available for real–life emergencies.  
Source: <http://www.wlbt.com/Global/story.asp?S=3448322>
22. *June 08, The Southern Illinoisan* — **Area agencies stage mock disaster at Illinois.** An imaginary bioterrorism scenario was played out Tuesday, June 7, at the Du Quoin State Fairground in southern Illinois to allow emergency personnel from throughout the region to practice and assess their response to a bioterrorism event, said David Searby Jr., operations officer for the Du Quoin Emergency Services and Disaster Agency. Those involved in Tuesday's drill did everything as they would have in the event of a real incident. In all, about 300 emergency response personnel and volunteers participated. The new Southern Illinois Center was utilized as an assessment and dispensing facility where those who were playing the parts of victims could go to receive the treatment that would have been antibiotics if they had actually been exposed. Local hospitals conducted drills, too, testing their response to people describing various symptoms. By the time the event wrapped up, Pinckneyville Community Hospital was simulating all beds being full and looking for backup at nearby hospitals.  
Source: <http://www.thesouthern.com/articles/2005/06/08/local/104027.txt>
23. *June 07, Washington Technology* — **Agency officials fine–tune emergency XML.** The Common Alerting Protocol (CAP) is a standard message format for emergency alerts and notifications. It is interoperable with many types of messaging software, making it easier to

send a single message to a variety of recipients quickly. The Emergency Interoperability Consortium, composed of government and industry emergency management groups as well as FEMA, wrote the protocol in 2003. It was adopted in 2004 by the Organization for Advancement of Structured Information Standards (Oasis), a standards-setting industry group. It is being implemented by numerous federal, state and local disaster management agencies. The CAP now has been updated to Version 1.1, and IT companies that support homeland security and public warning systems are invited to submit comments by July 15. In related developments, FEMA in January signed a memorandum of understanding with the consortium to develop additional Emergency Data Exchange Language (EDXL), a suite of XML standards that covers a broad variety of communications needs for emergency managers. The common alerting protocol is viewed as a component of EDXL. In addition to FEMA's initiatives, the Department of Homeland Security is sponsoring the National Information Exchange Model, based on the Global Justice XML data standards developed by the Justice Department with state and local law enforcement agencies. CAP document:

[http://www.oasis-open.org/committees/download.php/12649/CAPv 1-1.pdf](http://www.oasis-open.org/committees/download.php/12649/CAPv1-1.pdf)

Source: [http://www.washingtontechnology.com/news/1\\_1/daily\\_news/26370-1.html](http://www.washingtontechnology.com/news/1_1/daily_news/26370-1.html)

24. *June 07, Radio Iowa* — **Disaster simulated in Iowa city.** An exercise Monday, June 6, in Warren County, IA, brought first-responders to the hot-air balloon launching field on the city of Indianola's east side. Indianola Fire Chief Brian Seymour said emergency administrators putting together this kind of mock disaster exercise looked at what others around Iowa have done. There are some planning tools for them to study and review. He says they also looked at the stories of other communities that have coped with real emergencies. They offer the reports on what worked for them and what didn't, so others can learn from their experience. Fire fighters from Indianola and surrounding communities struggled in nearly 90-degree heat, as they coped with an imaginary scenario that had 45 to 50 victims of a car-crash type situation. The chief says triage was one main focus, sorting out the most urgent cases and dealing with them quickly so the fire and rescue crews will have their plans rehearsed when a real disaster faces them.

Source: <http://www.radioiowa.com/gestalt/go.cfm?objectid=2A842DE7-D923-4BFC-BB6205D69933F8C9>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

25. *June 07, FrSIRT* — **FlatNuke multiple input validation vulnerabilities.** Multiple input validation vulnerabilities reportedly affect FlatNuke. These issues are due to a failure of the application to properly sanitize user supplied input prior to using it in application critical actions such as generating Web content or loading scripts. An attacker may leverage these issues to execute arbitrary PHP code, execute client side script code in the browsers of unsuspecting users through cross site scripting attacks, and gain access to sensitive information. Other attacks are also possible. Upgrade to FlatNuke version 2.5.4:

[http://sourceforge.net/project/showfiles.php?group\\_id=93076&package\\_id=98622](http://sourceforge.net/project/showfiles.php?group_id=93076&package_id=98622)

Source: <http://www.frsirt.com/english/advisories/2005/0697>

*June 07, eWeek* — **FCC chairman outlines deregulatory agenda.** Federal Communications Commission (FCC) Chairman Kevin Martin, who took the helm of the agency this spring, on Tuesday, June 7, outlined an agenda that will extend the deregulatory program of his predecessor, Michael Powell. Addressing the telecommunications industry at its annual gathering, the Supercomm conference and expo in Chicago, Martin said his top priority is to create a regulatory environment conducive to furthering broadband deployment—a priority of the Bush Administration as well. Emphasizing that part of the FCC's job is to "level the playing field" for telecom providers, Martin said the commission will continue to promote a light touch when it comes to implementing regulations. In the wireless realm, the commission will likely move toward less regulation as well. To facilitate continued wireless growth, the agency will make more spectrum available with limited rules on its use. Policymakers need to re-examine the traditional mode of regulating communications based on the type of network (e.g., cable, wireline, wireless) used to deliver services, but there are many decisions that the agency can make under the current structure, Martin said.

Source: <http://www.eweek.com/article2/0,1759,1825464,00.asp>

27. *June 07, NewScientist* — **Quantum cryptography network gets wireless link.** The world's first quantum encryption computer network has been expanded to include a wireless link that uses quantum communications codes. The wireless connection was added to the Defense Advanced Research Projects Agency (DARPA) Quantum Network, a quantum fiber-optic network buried beneath the ground in Massachusetts. The network was built by BBN Technologies with funding from DARPA. It now links ten different sites, including BBN's offices, Harvard University and Boston University. Most modern cryptography rests upon the difficulty of solving very complex mathematical problems used to encrypt data. This makes it theoretically vulnerable to being hacked using dramatic mathematical or computing breakthroughs. By contrast, quantum cryptography near guarantees communications security, using quirks of quantum physics to thwart eavesdropping attempts. Quantum cryptography guarantees security by encoding information as polarized photons which can be sent down a fiber optic cable or through the air. Intercepting these photons disturbs their quantum state, alerting both sides to an eavesdropper's presence.

Source: <http://www.newscientist.com/article.ns?id=dn7484>

28. *June 06, SecurityFocus* — **PortailPHP ID parameter SQL injection vulnerability.** PortailPHP is prone to an SQL injection vulnerability. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. No solution is currently available.

Source: <http://www.securityfocus.com/bid/13708/exploit>

### Internet Alert Dashboard

DHS/US-CERT Watch Synopsis Current Port Attacks	
Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 6881 (bittorrent), 27015

(halflife), 1026 (----), 139 (netbios-ssn), 53 (domain),  
32775 (sometimes-rpc13), 1434 (ms-sql-m), 80 (www)

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

29. *June 03, ABC (NC)* — **New high-tech security at education building.** Imagine entering a building, having your ID scanned, then being issued an ID badge complete with a bar code. This high-tech security system is now in place at the Public Instruction Building in downtown Raleigh, NC. Ben Matthews, the Director of School Support, says they've been using the Lobbyguard System for the past two months. "We can take a picture of someone which can actually be a real deterrent." The Lobbyguard System is not only used at the Education Building but it is also used in several Wake County, NC, schools. "In our school settings if someone's trying to sign into the system and they're on a sex offender list then it will stop the process and notify the appropriate person to prevent someone from signing in." During a recent fire drill, administrators used the system to make sure everyone on the list was accounted for and safe. Source: [http://abclocal.go.com/wtvd/news/060305\\_NW\\_lobbyguardsecurity.html](http://abclocal.go.com/wtvd/news/060305_NW_lobbyguardsecurity.html)

[\[Return to top\]](#)

## **General Sector**

30. *June 07, Associated Press* — **Four men detained in possible terror cell.** Federal authorities have detained four men who they believe are linked to an al Qaeda terror cell in Lodi, CA. Hamid Hayat, 22, and his father, Umer Hayat, 47, were arrested over the weekend on charges of lying to federal agents and both made a brief appearance in U.S. District Court in Sacramento, CA, on Tuesday, June 7, FBI special agent John Cauthen confirmed to The Associated Press. The two men, who are both U.S. citizens, are being held in Sacramento County Jail. Shabbir Ahmed and Mohammed Adil Khan, are being detained on immigration violations, Cauthen said. According to a federal criminal complaint filed in Sacramento court, where the Hayats had an initial appearance on Tuesday, Hamid Hayat is accused of training in an al Qaeda camp in Pakistan to learn "how to kill Americans." The younger Hayat is accused of being trained to use explosives and other weapons, using photographs of President Bush as targets. Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/06/07/state/n222457D69.DTL>

[\[Return to top\]](#)

## **DHS/IAIP Products & Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

**DHS/IAIP Daily Open Source Infrastructure Reports** – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

**Homeland Security Advisories and Information Bulletins** – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: <http://www.dhs.gov/dhspublic/display?theme=70>

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS/IAIP Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS/IAIP Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS/IAIP**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.